TESTIMONY OF ANDY BECHTOLSCHEIM
VICE PRESIDENT AND GENERAL MANAGER
GIGABIT SYSTEMS BUSINESS UNIT
CISCO SYSTEMS, INC.
BEFORE THE SENATE COMMITTEE ON
COMMERCE, SCIENCE AND TRANSPORTATION
FEBRUARY 28, 2002

Good morning and thank you, Mr. Chairman, for convening these hearings on protecting digital content and promoting broadband deployment. At Cisco, we believe that growing the Internet from the current narrowband generation of email and web browsing to one that is capable of delivering movies and multimedia applications is crucial to the economic future of our country. Although many forces will drive broadband deployment, one key factor will be the availability of audiovisual content on the Internet. The more and better content that is available on the Internet, the more consumers will choose broadband connections to access that content and also gain access to the benefits of broadband in other areas, such as education, medicine, and government services.

But why should government care about the deployment of broadband Internet networks? The answer is simple, yet compelling. Broadband enables new applications and services that will continue the radical transformation of our economy that the Internet has begun. It is not just about watching movies online or playing interactive games, however interesting those activities may be. It is about improving the productivity of our workforce and increasing long term economic growth. If we look at the recent past, we can see the enormous impact of first generation Internet services on the economy. In industries where information technology and Internet services were integrated into their operations, productivity increased four times faster than in industries that did not integrate information technology. Higher productivity growth creates more jobs, strengthens existing industries, and provides higher wages for workers.

But as I said before, movies will help draw consumers to broadband services. But first, the movies must be drawn to the Internet. The motion picture industry is certainly interested in using the Internet as a new distribution platform for its movies. But the movie industry is not interested in doing so without proper protection against unauthorized copying of copyrighted material. We would not expect anyone to put their money in a bank that does not have a safe and secure vault to store the money. Likewise, it is not reasonable to expect movie studios to release content on the Internet without strong copy protection systems in place. The technology industry, including Cisco, has worked hard to create copy protection technology and continues to work with the content industry to improve and implement such technologies.

Copy protection technology, however, must be about more than just preventing authorized copying of content. The technology must support multiple encoding technologies, multiple platforms, and multiple categories of devices. Most importantly, the technology must be consumer friendly. If consumers find the copy protection technology to be confusing, difficult and burdensome, they will not move to the new services. For consumers to embrace broadband distribution of movies, copy protection must be transparent to the user, available for multiple platforms and formats, and support multiple usage models such as purchase, rental, subscription and broadcast.

The best example of this type of security is already in widespread use on the Internet today. Millions of consumers make secure transactions on the Internet using the Secure Socket Layer encryption technology, commonly referred to as SSL. The open and interoperable SSL technology allows for the transmission of sensitive data, such as credit card numbers, securely across the Internet in a manner that is virtually transparent to the user. In fact, most Internet users do not even know that they are using SSL protection in making these transactions. The creation of SSL was critical to developing commerce on the Internet largely because it is an open and interoperable system that supports almost all technologies and is easy for consumers to use.

It became clear that a similar system for protecting content on the Internet would be the best and most consumer friendly way to bring high value content to the Internet. So Cisco took up this task and has created a system called Open Conditional Content Access Management, or OCCAM. OCCAM is an end-to-end protocol for protecting content from unauthorized copying, distribution and playback and can be used to protect content during transmission and storage in any public, private or home network.

OCCAM utilizes 128-bit AES or Advanced Encryption Standard for encrypting content. This is one of the best encryption technologies known today which was created by industry working with the National Institute of Standards at the Department of Commerce. In addition, OCCAM uses PKE or Public Key Encryption which allows for the secure transmission of a content key from a content provider to the consumer playback device. Both of these technologies have been extensively researched, are in wide use on the Internet today, and are considered open standards.

I would like to state for the record that government, in particular the Department of Commerce has already greatly contributed to enabling content protection technology, by defining the standards for security technologies that are used as the basis for ecommerce,.

In order to maintain the open nature of this system, Cisco has created a non-profit licensing organization to administer the OCCAM technology. The licensing organization can also be used to enforce the robust implementation of the copy protection technology by manufacturers of compliant equipment. Cisco believes that the open licensing of open and interoperable technology will be the best means of creating strong and consumer friendly content protection to encourage the distribution of content on the Internet.

The availability of open systems of content protection like OCCAM, which can be enforced through licensing regimes leads to the conclusion that legislation prescribing specific content protection technology, is not necessary. In fact, it would be quite undesirable. If the decision on selecting and implementing technologies were left to government bureaucrats, we run the risk of selecting inferior, market-unfriendly, and limited technologies. We would also limit future innovation in security technology by freezing in place current technology and only making changes at the speed of government, not the speed of the Internet.

Looking at history only confirms this conclusion. For example, the Audio Home Recording Act attempted to legislatively protect digital audio content through a government-mandated copy control technology. Initially, the AHRA largely succeeded only in destroying the market for digital audio devices. Then, as technology developed, it became clear that the copy protection system of the AHRA was extremely ineffective. Despite provisions in the AHRA that would allow the mandated technology to be "updated," no serious attempt has been made to do so. Instead, the recording industry is working through private sector technologies to solve its problems, rather than seeking another government mandate.

The best way to protect content is through technology, not government. Proven content protection technology exists today that does not require new legislation for efficacy. Alternative technologies that would require new legislation to be effective in our opinion are not technically sound because the protection offered by the law can never be as strong as protection offered by the strength of encryption and mathematics.

A standard for copy protection is required to assure a viable market for content creators and consumer electronics companies, while making the widest range of content available to the public. Such a standard should be technically sound, be open to all qualfied participants, and not be controlled by a for-profit entity. Cisco remains committed to work with the industry to implement an open and interoperable system of this nature.

Mr. Chairman, thank you for the opportunity to present Cisco's views today.